UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,113	10/15/2001	Eng-Whatt Toh	23615-05502	3747

7590 05/31/2006

ROBERT N . BLACKMAN
MEREK , BLACKMORE & VOORHEES , LLC
673 S . WASHINGTON ST .
ALEXANDRIA, VA 22314

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/978,113	TOH ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/7/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-68* is/are pending in the application.

4a) Of the above claim(s) *23-32* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 33-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/10-3-2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 23-32 are cancelled. Applicant's arguments/amendments with respect to amended claim 2, previously presented claims 1 & 3-53, and newly presented claims 54-68 filed 3/7/2006 have been fully considered and therefore the claims are rejected under new grounds as necessitated by the Applicant's submission of an information disclosure statement filed October 3, 2005. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Objections

Claims 2, 59, and 64 are objected to for minor informalities.

As per claim 2:

Claim 2 is objected to because of the following informalities: line 5 of the claim contains the word "encrypted" which is the misspelled form of "encrypted." Appropriate correction is required.

As per claim 59:

Claim 59 is missing.

As per claim 64:

Claim 64 is objected to because of the following informalities: line 5 of the claim contains a ';' instead of a '.' where no other limitations follow after the semi-colon. Appropriate correction is required.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-5, 7-10, 12-18, 20-22, 39-43, 45-48, 50-58, and 60-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,338,140 and further in view of Boebert et al., US Patent No. 5,864,683.

As per claims 1 and 39:

Owens et al. substantially teach a computer-implemented method/computer readable medium comprising a switch system performing the steps of: associating each of a plurality of access systems with a key derived from another key, i.e. a key pair, associated with said access system (col. 2, lines 27-39); in response to a request from a first access system to transmit data to a second access system: authenticating the first access system using the derived key associated with the first access system (col. 13, lines 13-34); forming a first network connection between the authenticated first access system and the switch system (col. 9, lines 55-67 and col. 10, lines 1-2 and 13-16); accepting data from the authenticated first access system via the first network connection (col. 10, lines 13-16).

Not explicitly disclosed is authenticating the first/second access system using the public key associated with the first/second access system. However, Boebert et al. teach that the use of public key cryptography allows for a secure authentication process for workstations that are connecting to any public network, such as the Internet, for communication purposes. Therefore,

it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. to authenticate both the first and second access systems using their associated public keys in order to authenticate the access systems to ensure that only the systems with proper access rights gain information through the communications. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using public-key cryptography in public networks is necessary as there is a need for a stronger means of authentication in a global network in col. 6, lines 42-55 and col. 28, lines 47-67.

Also not explicitly disclosed is forming a first/second cryptographically secure network connection between the authenticated first/second access system and the switch system and transmitting the data to the authenticated second access system via the second cryptographically secure network connection. However, Boebert et al. teach that once the access systems are authenticated each with respect to a switch station, a secure communication can be established so that the data may be indirectly transmitted from a first access point to a second access point, each via a secure channel that has been established with regards to their authentication procedures. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. to form two cryptographically secure network connections between the switch system and each of the access points and to only send the data when that second secure channel has been established (indicating that the second access point was properly authenticated). This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated

to do so since Boebert et al. suggest that using a secure communications path ensures that the information viewed or sent to subsystems are not copied or modified along the way in col. 6, lines 42-55 and col. 11, lines 20-35.

As per claim 2:

Owens et al. and Boebert et al. substantially teach the method of claim 1. Furthermore, Boebert et al. teach wherein the switch system issues to an access system the access system's private-pubic key pair and the switch system authenticates the first access system using the private key associated with the first access system an successfully decrypting the document using the public key associated with the first access system (col. 13, line 55 – col. 14, line 14).

As per claims 3 and 41:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 1 and 39. Further, Owens et al. teach an authentication scheme occurring in a mobile switching center connected to various nodes equipped with a cryptographic algorithm (col. 3, lines 4-9).

As per claims 4 and 42:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 2 and 41. Furthermore, Boebert et al. teach wherein the first and second access systems connect to the switch system via different nodes (col. 11, lines 20-35).

As per claims 5 and 43:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 1 and 39. Furthermore, Boebert et al. teach comprising the switch system performing the step of: using a switch system private key, in conjunction with an access system using a

corresponding switch system public key, to authenticate the switch system to the access system (col. 11, lines 20-35).

As per claims 7 and 45:

Owens et al. and Boebert et al. teach the method/computer readable medium of claims 6 and 44. Furthermore, Boebert et al. teach wherein the first and second cryptographically secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key (col. 11, lines 20-35).

As per claims 8 and 46:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 1 and 39. Furthermore, Boebert et al. teach wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key (col. 12, lines 21-27).

As per claims 9 and 47:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 1 and 39. Furthermore, Boebert et al. teach wherein the data comprises at least one from the group comprising: a digest of at least a portion of the data; and a digital signature of the first access system (col. 4, lines 53-63).

As per claim 10:

Owens et al. and Boebert et al. substantially teach the method of claim 1. Furthermore, Boebert et al. teach the method comprising the switch system performing the step of storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital

signature (col. 4, lines 53-63).

As per claim 12:

Owens et al. and Boebert et al. substantially teach the method of claim 1. Further, Owens teach that two gateways are required, one for each TCP/IP network to IS-41 network interface where the authentication engine according to the instant invention may be connected to either or both such access gateways, converting the message into an IS-41 message and sends it to a mobile switching center (col. 19, lines 16-36).

As per claim 13:

Owens et al. and Boebert et al. substantially teach the method of claim 1. Further, Owens teach access gateways, converting the message into an IS41 message and sends it to a mobile switching center which routes the message to the base station, which transmits the message to the mobile station (col. 19, lines 16-36). The base station acts as an application proxy.

As per claim 14:

Owens et al. and Boebert et al. substantially teach the method of claim 13. Further, Owens teach a cryptographic algorithm utilizing numerical inputs and produce numerical outputs (col. 19, lines 61-64). The algorithm acts as an application proxy processing data based upon a define series of steps.

As per claim 15:

Owens et al. and Boebert et al. substantially teach the method of claim 14. Not explicitly disclosed is wherein the policies for the application proxy are set by the access system. However, Boebert et al. teach that the access system is in charge of establishing and maintaining the system in such a way that the security policies are not violated. Therefore, it would have been

obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the access system to set the security policies for the application proxy. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that correctly setting the security policy for the application proxy will ensure that violations of the system do not occur in col. 11, line 56 – col. 12, line 27.

As per claim 16:

Owens et al. substantially teach a switch system for establishing a secure network connection between at least two access systems, the switch system comprising: at least one node comprising: a key module for associating each access system with a key derived from another key, i.e. a key pair, associated with said access system (col. 2, lines 27-39); in response to a request from a first access system to transmit data to a second access system: authenticating the first access system using the derived key associated with the first access system (col. 13, lines 13-34); forming a first network connection between the authenticated first access system and the switch system (col. 9, lines 55-67 and col. 10, lines 1-2 and 13-16); accepting data from the authenticated first access system via the first network connection (col. 10, lines 13-16).

Not explicitly disclosed is an authentication module, coupled to the key manager module, for using an access system's public key, in conjunction with the access system using its private key, to authenticate the access system. However, Boebert et al. teach that the use of public key cryptography allows for a secure authentication process for workstations that are connecting to any public network, such as the Internet, for communication purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method

disclosed in Owens et al. to authenticate both the first and second access systems using their associated public keys in order to authenticate the access systems to ensure that only the systems with proper access rights gain information through the communications. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using public-key cryptography in public networks is necessary as there is a need for a stronger means of authentication in a global network in col. 6, lines 42-55 and col. 28, lines 47-67.

Also not explicitly disclosed is a secure network module, coupled to the authentication module, for establishing a cryptographically secure network connection between the switch system and an authenticated access system, whereby data is received from a first access system via a first secure connection and transmitted to a second access system via a second secure connection. However, Boebert et al. teach that once the access systems are authenticated each with respect to a switch station, a secure communication can be established so that the data may be indirectly transmitted from a first access point to a second access point, each via a secure channel that has been established with regards to their authentication procedures. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. to form two cryptographically secure network connections between the switch system and each of the access points and to only send the data when that second secure channel has been established (indicating that the second access point was properly authenticated). This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using a secure communications path ensures that the information

viewed or sent to subsystems are not copied or modified along the way in col. 6, lines 42-55 and col. 11, lines 20-35.

As per claim 17:

Owens et al. and Boebert et al. substantially teach the system of claim 16. Furthermore, Boebert et al. teach wherein the key module is further adapted to perform the step of: issuing a private-public key pair to an access system (col. 12, lines 28-32).

As per claim 18:

Owens et al. and Boebert et al. substantially teach the system of claim 16. Furthermore, Boebert et al. teach wherein the authentication module is further adapted to perform the step of: using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system (col. 11, lines 20-35).

As per claim 20:

Owens et al. and Boebert et al. substantially teach the system of claim 19. Furthermore, Boebert et al. teach wherein the cryptographically secure network connections are formed using at least one encryption key from the group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key (col. 11, lines 20-35).

As per claim 21:

Owens et al. and Boebert et al. substantially teach the system of claim 16. Furthermore, Boebert et al. teach wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key (col.

12, lines 21-27).

As per claim 22:

Owens et al. and Boebert et al. substantially teach the system of claim 16. Furthermore, Boebert et al. teach wherein the node further comprises: a computer-readable medium for storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of an access system (col. 4, lines 53-63).

As per claim 40:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 39. Furthermore, Boebert et al. teach wherein the key module is further adapted to perform the step of: issuing a private-public key pair to an access system (col. 12, lines 28-32).

As per claim 48:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 39. Furthermore, Boebert et al. teach comprising program code adapted to perform the step of: storing at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature (col. 4, lines 53-63).

As per claim 50:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 39. Furthermore, Boebert et al. teach wherein the switch system interfaces with an application which utilizes the data exchanged between the first and second access systems (col. 12, line 28-40).

As per claim 51:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 39. Further, Owens teach access gateways, converting the message into an IS41 message and sends it to a mobile switching center which routes the message to the base station, which transmits the message to the mobile station (col. 19, lines 16-36). The base station acts as an application proxy.

As per claim 52:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 51. Not explicitly disclosed is wherein the application proxy processes data initiated from an access system and data intended for the access system based upon predefined policies. However, Boebert et al. teach that the access system is in charge of establishing and maintaining the system in such a way that the security policies are not violated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the access system to set the security policies for the application proxy. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that correctly setting the security policy for the application proxy will ensure that violations of the system do not occur in col. 11, line 56 – col. 12, line 27.

As per claim 53:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 52. Not explicitly disclosed is wherein the policies for the application proxy are set by the access system. However, Boebert et al. teach that the access system is in charge of establishing and maintaining the system in such a way that the security policies are not violated. Therefore, it

would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the access system to set the security policies for the application proxy. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that correctly setting the security policy for the application proxy will ensure that violations of the system do not occur in col. 11, line 56 – col. 12, line 27.

As per claim 54:

Owens et al. substantially teach a method comprising a switch system performing the steps of: associating each of a plurality of access systems with a key derived from another key, i.e. a key pair, associated with said access system (col. 2, lines 27-39); in response to a request from a first access system to transmit data to a second access system: authenticating the first access system using the derived key associated with the first access system (col. 13, lines 13-34); forming a first network connection between the authenticated first access system and the switch system (col. 9, lines 55-67 and col. 10, lines 1-2 and 13-16); accepting data from the authenticated first access system via the first network connection (col. 10, lines 13-16).

Not explicitly disclosed is authenticating the first/second access system by decrypting a message encrypted by the first access system using one key of a private-public key pair associated with the first/second access system. However, Boebert et al. teach that the use of public key cryptography allows for a secure authentication process for workstations that are connecting to any public network, such as the Internet, for communication purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. to authenticate both the first and second access systems

using their associated public keys in order to authenticate the access systems to ensure that only the systems with proper access rights gain information through the communications. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using public-key cryptography in public networks is necessary as there is a need for a stronger means of authentication in a global network in col. 6, lines 42-55 and col. 28, lines 47-67.

Also not explicitly disclosed is forming a first/second cryptographically secure network connection between the authenticated first/second access system and the switch system, wherein communications are encrypted by one key of the private-public key pair and transmitting the data to the authenticated second access system via the second cryptographically secure network connection. However, Boebert et al. teach that once the access systems are authenticated each with respect to a switch station, a secure communication can be established so that the data may be indirectly transmitted from a first access point to a second access point, each via a secure channel that has been established with regards to their authentication procedures. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. to form two cryptographically secure network connections between the switch system and each of the access points and to only send the data when that second secure channel has been established (indicating that the second access point was properly authenticated). This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using a secure communications path ensures that the information

viewed or sent to subsystems are not copied or modified along the way in col. 6, lines 42-55 and col. 11, lines 20-35.

As per claim 55:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Boebert et al. teach wherein the key module is further adapted to perform the step of: issuing a private-public key pair to an access system (col. 12, lines 28-32).

As per claim 56:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Owens et al. teach wherein the switch system comprises a plurality of nodes securely networked together (col. 3, lines 4-9).

As per claim 57:

Owens et al. and Boebert et al. substantially teach the method of claim 56. Furthermore, Boebert et al. teach wherein the first and second access systems connect to the switch system via different nodes (col. 11, lines 20-35).

As per claim 58:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Boebert et al. teach the method comprising the switch system performing the step of: using a switch system private key, in conjunction with an access system using a corresponding switch system public key, to authenticate the switch system to the access system (col. 11, lines 20-35).

As per claim 60:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claim 58. Furthermore, Boebert et al. teach wherein the first and second cryptographically

secure network connections are each formed using at least one encryption key from a group comprising a symmetric key, an asymmetric key, and a symmetric session key encrypted with an asymmetric key (col. 11, lines 20-35).

As per claim 61:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Boebert et al. teach wherein the data is encrypted with at least one encryption key for which the switch system does not have access to the encryption key's corresponding decryption key (col. 12, lines 21-27).

As per claim 62:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Boebert et al. teach wherein the switch authenticates the first access system by decrypting a message encrypted by the first access system using the first access system's private-public key pair (col. 13, line 55 – col. 14, line 14).

As per claim 63:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Boebert et al. teach wherein the switch authenticates the second access system by decrypting a message encrypted by the second access system using the second access system's private-public key pair (col. 13, line 55 – col. 14, line 14).

As per claim 64:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Not explicitly disclosed is wherein the switch forms a first cryptographically secure network connection between the authenticated first access system and the switch system, wherein communications

are encrypted by the first access system private-public key pair. However, Boebert et al. teach that public key cryptography is used in systems where the communications are over the Internet and that each of the clients must first be authenticated by checking a message that is encrypted with the key of the access system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the communications to be encrypted by the first access system private-public key pair which is used for authentication. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using encrypted communications protects the data being transmitted in col. 11, lines 20-35 and col. 14, lines 1-14.

As per claim 65:

Owens et al. and Boebert et al. substantially teach the method of claim 55. Not explicitly disclosed is wherein during transmission the data to be authenticated to the second access system via the second cryptographically secure network connection is encrypted by said second access system public key pair. However, Boebert et al. teach that public key cryptography is used in systems where the communications are over the Internet and that each of the clients must first be authenticated by checking a message that is encrypted with the key of the access system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the communications to be encrypted by the second public key pair which is used for authentication on the receiving side as well. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest

that using encrypted communications protects the data being transmitted in col. 11, lines 20-35 and col. 14, lines 1-14.

As per claim 66:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Not explicitly disclosed is wherein during transmission the data to be authenticated to the second access system via the second cryptographically secure network connection is encrypted by said second access system public key pair. However, Boebert et al. teach that public key cryptography is used in systems where the communications are over the Internet and that each of the clients must first be authenticated by checking a message that is encrypted with the key of the access system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the communications to be encrypted by the second public key pair which is used for authentication on the receiving side as well. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using encrypted communications protects the data being transmitted in col. 11, lines 20-35 and col. 14, lines 1-14.

As per claim 67:

Owens et al. and Boebert et al. substantially teach the method of claim 65. Furthermore, Owens et al. teach wherein said plurality of access systems, each has a unique private-public key pair associated with said access system (col. 2, lines 27-39).

As per claim 68:

Owens et al. and Boebert et al. substantially teach the method of claim 54. Furthermore, Owens et al. teach that all of the information goes through the switching center for authentication, regardless of which direction the request is coming from (col. 19, lines 25-36). Not explicitly disclosed is wherein communications are encrypted by the switch system private-public key pair. However, Boebert et al. teach that encrypting data that is being communicated over a public network should be encrypted for confidentiality purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Owens et al. for the communications to be encrypted by the switch system's public key pair. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Boebert et al. suggest that using encrypted communications protects the data being transmitted in col. 4, lines 53-67.

III. Claims 6, 19, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Owens et al., US Patent No. 6,338,140 and Boebert et al., US Patent No. 5,864,683 as applied to claims 1, 16, and 39 above, and further in view of Stevens, (1994).

As per claims 6 and 44:

Owens et al. and Boebert et al. substantially teach the method/computer readable medium of claims 1 and 39. Not explicitly disclosed is the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model. However, Stevens teach protocols are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7,

"Layering"). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

As per claim 19:

Owens et al. and Boebert et al. substantially teach the system of claim 16. Not explicitly disclosed is the first and second cryptographically secure connections are each implemented by encrypting the data at a layer selected from the group comprising an application layer, a presentation layer, and a session layer of the Open Systems Interconnection reference model. However, Stevens teach protocols are normally developed in layers, with each layer responsible for a different facet of the communications (pg. 1-7, "Layering"). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. by including processes at different layers. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Stevens, in order to process data in a modular fashion, thus allowing for quick and easy program alterations to occur.

IV. Claims 11 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,338,140 and Boebert et al., US Patent No. 5,864,683, as applied to claims 10 and 48 above, and further in view of Rowney et al., US Patent No. 5,987,140.

As per claim 11:

Owens et al. and Boebert et al. substantially teach the method of claim 10. Not explicitly disclosed is compromising the switch system performing the step of time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system. However, Rowney teach a merchant computer system calculates a digital signature for the combined contents of the combined block comprising basic capture response and the signature public key certificate and appends the signature to the combination of the combined basic authorization request and the signature public key certificate (col. 18, lines 55-65). The digital signature may very well contain a time-stamp. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to form a digest containing all the pertinent information related to a message sent by the first access system.

As per claim 49:

Owens et al. and Boebert et al. substantially teach the computer readable medium of claim 48. Not explicitly disclosed is further comprising program code adapted to perform the step of: time-stamping at least one of the group comprising the data, a digest of at least a portion of the data, and a digital signature of the first access system. However, Rowney teach a merchant computer system calculates a digital signature for the combined contents of the combined block comprising basic capture response and the signature public key certificate and appends the signature to the combination of the combined basic authorization request and the signature public key certificate (col. 18, lines 55-65). The digital signature may very well contain

a time-stamp. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Owens et al. to include time-stamping a group. This modification would have been obvious to a person having ordinary skill in the art. One skilled in the art would have been motivated to do so, as suggested by Rowney, in order to form a digest containing all the pertinent information related to a message sent by the first access system.

Conclusion

Applicant's submission of an information disclosure statement under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p) on 10/3/2005 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
5/30/2006

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100